IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

CENTRIPETAL NETWORKS, INC., Plaintiff, v. CISCO SYSTEMS, INC., Defendant.	CIVIL ACTION NO. 2:18cv94

TRANSCRIPT OF VIDEOCONFERENCE BENCH TRIAL PROCEEDINGS

Norfolk, Virginia

May 6, 2020

Volume 1B
Pages 94-164

BEFORE: THE HONORABLE HENRY COKE MORGAN, JR.
United States District Judge

APPEARANCES:

KRAMER LEVIN NAFTALIS & FRANKEL LLP
By: Paul J. Andre
Counsel for the Plaintiff

DUANE MORRIS LLP
By: Matthew C. Gaudet
Counsel for the Defendant

I N D E X

E X H I B I T S

(None offered)

(Proceedings resumed at 2:13 p.m.)

THE COURT: All right, counsel. Are we ready to resume?

MR. GAUDET: Yes, we are, Your Honor.

THE COURT: Okay.

KEVIN C. ALMEROTH, Ph.D., called by the Defendant, having been first duly sworn, was examined and testified as follows:

TECHNOLOGY TUTORIAL OF DEFENDANT (Resumed)

BY MR. GAUDET:

Q. Thank you. And we were getting towards the end of the first of the four sort of modules in our tutorial.

So, Dr. Almeroth, if you would resume with the tutorial of the kind of overview of basic networking.

A. Certainly. So we had talked about headers in the packet and some of the details, and we talked a little bit about payloads. On slide 12 I have an additional animation that really gets at what I think is a fairly straightforward concept now, which is that if you have a file that you want to be able to send across the network, that that file is divided up into a series packets, and each of those packets will have a header, and each will have a portion of the original file.

So, for example, if you have a PDF file of a decision that you wanted to send across the network, it would

be --

THE COURT: What does PDF mean?

THE WITNESS: I'm sorry. It's a data format for how you would represent your decision, so that --

THE COURT: Payload data format? Is that what that means?

THE WITNESS: It's been a while. I actually don't remember.

But it's a file that you can -- I guess after a while, you stop caring what the underlying words are.

MR. GAUDET: Your Honor, we've got a small army of engineers, and nobody came up with a better acronym than you did.

MR. ANDRE: Portable data format.

MR. GAUDET: There you go. If I were Mr. Andre, I would have let it go.

THE COURT: Well, I keep seeing "PDF" on my cell phone, and I never knew what it meant. It means portable what?

THE CLERK: It means postscript data format. Postscript data format.

THE COURT: Postscript data format.

THE CLERK: According to Anna Paretti, postscript data format.

THE COURT: Well, can we get that person in here as

an expert witness?

THE CLERK: She is listening and chatted the answer.

THE COURT: Okay. All right. Let's go ahead.

BY MR. GAUDET:

Q. And, Dr. Almeroth, in practical terms, when you get a document by e-mail and it's -- for example, it's something that you could have printed out in hard copy, for example, a copy of a court's opinion, is that format typically what we just referred to as PDF?

A. Yes, it is.

Q. Okay. If you would, proceed.

A. Sure. So the document is divided up into a series of packets, and then those packets are sent across the network.

Packets generally have about 1500 characters, and so you can think about how many packets it would take to divide up a document like a court decision and put that across the network. It would be thousands of packets. And so, really, the point of the Internet here is that it has many packets that are being delivered between sources and destinations.

THE COURT: Is there a maximum size of a packet?

THE WITNESS: There is. There are a couple of different maximums that can apply. For an Internet protocol packet, it's about 65,000 characters, but, in practice, networks that deliver IP packets, Internet protocol packets, usually about 1500 bytes.

THE COURT: It's usually about 1500, but it can go up to -- how much did you say?

THE WITNESS: 65,000.

THE COURT: 65,000. Does it have to be a minimum size to justify being a separate packet?

THE WITNESS: No. You could send one character. Sometimes, if you have a chat application and you type a character and the character shows up on the screen, you could send one byte over the Internet as a packet, one character.

THE COURT: Okay. So this packet is usually about 1500 bytes? Is that the right word?

THE WITNESS: Yes, sir, and a byte is really like a character or a number.

THE COURT: That's the same as a character?

BY MR. GAUDET:

Q. Would that just be a 1 or a 0?

A. No. A byte is 8 bits. A bit is a 1 or a 0.

THE COURT: A bit and a byte. Okay. May go up to 65,000 --

THE WITNESS: Yes, sir.

THE COURT: -- bytes.

THE WITNESS: Yes, sir.

THE COURT: Which would be 260,000 bits.

THE WITNESS: 256,000.

THE COURT: Okay.

THE WITNESS: It's usually multiples of two, because they are 1's and 0's, and that's how you represent them.

THE COURT: Okay. All right.

MR. GAUDET: You may have seen that I now have the distinction of being the first lawyer to ask his tutorialist a question and be told, "No."

BY MR. GAUDET:

Q. With that, Dr. Almeroth, if you would proceed.

A. Yes. So the next slide I will go over very quickly. It's about encryption, and I think Dr. Medvidovic was correct in describing that in some cases you would want to encrypt the data.

So here we have a file that will be divided into a series of packets. I'll show one of those packets going -- you know, ready to leave that first computer, and that payload portion, which would be a series of 1's and 0's, would be encrypted with a key. And so, that way, if somebody were looking at the network, they would see the payload, but they wouldn't be able to determine anything meaningful from that. You would still be able to see the header, as Dr. Medvidovic described, but the point would be that while that packet was being sent across the network, that payload would be encrypted.

Now, the receiver would have a key and would be able to unlock or decrypt the data and be able to see what the

sender had originally sent.

THE COURT: All right. So there would be no reason to send it encrypted unless somebody could unencrypt it.

THE WITNESS: That's correct.

THE COURT: So the person to whom it's directed, what do we call him?

THE WITNESS: The recipient, the receiver.

THE COURT: Okay.

BY MR. GAUDET:

Q. And to pick up on the Court's point, Dr. Almeroth, in order to be sure that both sides can actually decrypt this, is there yet another protocol or kind of a handshake that goes on beforehand to know that both sides are on the same page?

A. Yes. So you mentioned a protocol, and the name of the protocol could be something like a transport layer security protocol. And it's defined by the IETF, the Internet Engineering Task Force, and it tells you the rules for how a sender and a receiver would make sure that they were able to encrypt and decrypt the data.

THE COURT: Would a password be sufficient to unencrypt it?

THE WITNESS: Yes; obviously, if it's the right password.

THE COURT: All right. So if you get something and

you have to put in a password to retrieve it, that means that it's encrypted when it's sent to you. Is that right?

THE WITNESS: Yes, in usual circumstances.

THE COURT: Okay.

THE WITNESS: And I think the point that Dr. Medvidovic made, and I will make it as well, is that an increasing amount of traffic being sent across the Internet is encrypted. So it becomes a challenge for knowing whether or not packets that are encrypted actually contain malicious software or attacks.

THE COURT: They could just be something that is thought to be private. Like, for example, I get things on my iPhone from various sources, and they want to know the password, which I can't remember so I can't get it, so -- but that doesn't mean it's malicious. It could be just private, not malicious.

THE WITNESS: That's correct.

THE COURT: Well, how do you tell the difference?

THE WITNESS: That is the challenge, and that's what security tools have to be able to do.

And I think you asked them some very specific questions about, well, maybe where the request for your password is coming from. If it's coming from Bank of America, that might be trusted. If it's coming from some unknown source in a foreign country, that might be something

worth investigating. And so the challenge of security tools is knowing how to look at information that comes across the network, even if it's encrypted, to be able to determine whether it's malicious or not.

BY MR. GAUDET:

Q. Dr. Almeroth, approximately how long have these various encryption protocols been in existence?

A. Decades, more than a decade.

Q. And this discussion we're having now about the good use of encryption -- for example, privacy versus the dangerous use of encryption -- has that discussion been going on that whole time, as well?

A. Yes, it has. Very clearly, once the Internet really started to grow to be used for things like business, commerce, it became important to be able to encrypt the data that was sent over the network, and these protocols have been around for 20 years.

Q. If you would, proceed.

A. Certainly. All right. So then the next piece is, then, that that file goes back into the computer and is decrypted.

What I wanted to do now is, on slide 14, go back to this figure that showed that in a network enterprise, there can be lots of packets flowing around the network, and given the millions of packets that can come from all of these different applications, it's important to try and put

together a sense of which packets are related to which other packets. So if you send a file from one computer to another, it would be useful to understand which packets were part of or related to that particular file.

Now, first of all, there's a definition for kind of the relationship of those packets, and it's called a packet flow. And a packet flow is really where you have a set of packets being sent over the network; for example, from user 2 to user 5, representing the encrypted packets of that file. And you want to be able to relate them to each other, and on the Internet there's a term for that called the flow, and the flow is really the packets between a sender and a receiver for a single connection. And so you can think about individual packets, and then you can also think about grouping sets of packets together into these flows.

THE COURT: Well, a flow means whether packets are received as a group or as just a single communication. How do you know when a flow stops?

THE WITNESS: It depends on what level you look at them. You can look at individual packets, or you can take a step back and try and organize all the packets that you're seeing into distinct flows.

BY MR. GAUDET:

Q. And, Dr. Almeroth, maybe to help bring some of this into further view, if you -- let's say you have a particularly

large document, for example, the proposed findings of fact and conclusions of law of the parties, that would be a lot of packets, right?

A. That would be.

Q. Okay. So as --

THE COURT: You wouldn't want to try to carry it.

MR. GAUDET: Your Honor, we learned our lesson on that one.

BY MR. GAUDET:

Q. If you broke that document up -- let's say it turned into -- making this up -- a hundred packets. Is that at least reasonable for the example?

A. Probably about a million packets, but, okay.

MR. GAUDET: Your Honor, there he goes again.

BY MR. GAUDET:

Q. So a million packets. Now, would those million packets stay in specific order, 1 through a million, as they travel around the network?

A. No. Here's the analogy that I use:

Let's say that I had a 10,000-page document and I wanted to send it through the post office, and, for some reason, I wanted to send an envelope with only one page in it. I would prepare 10,000 different envelopes. I would write the address on the outside, put a stamp on it, and I would dump these 10,000 envelopes into the post office. You

can use your imagination and envision that they probably all go to the post office, but they might get sorted into different bins, and the bins might go in different directions, and so they could just kind of flow through the post office as independent little pieces of information and take all sorts of different paths through the network.

Now, hopefully, they would all reach the destination, and one of the things that your computer would do, or what you would do, is you would try and reassemble all of these envelopes or packets to get the original document that had been divided up and sent. And so that's part of this process of what a computer does when it receives all of these individual packets.

THE COURT: Well --

THE WITNESS: But as a collection, those packets would be a flow.

THE COURT: Well, didn't we say that sometimes on the address there's a number?

THE WITNESS: Yes.

THE COURT: And you could number the packets.

THE WITNESS: That's correct.

THE COURT: So that way it would -- you could put them back together, or maybe the computer could put them back together.

THE WITNESS: It would. And you're not using the

acronym, but you're talking about a field in the protocol of the Transmission Control Protocol. It has what's called a sequence number, and those sequence numbers are assigned by the sender, and they're used by the receiver to put the packets back into the right order.

BY MR. GAUDET:

Q. Is it fair to say in our example the million or so packets will kind of set out on their own over the network and then have a meet-up point at the other computer, where that number will then be used by the other computer to put them back together?

A. That's correct.

Q. And then this concept of a flow is just referring to that set of packets that together will eventually add up to that single document?

A. That's correct. And that right box -- there's a way of identifying and distinguishing one flow from another flow. So there's the source address that's sending the computer. There's a source port number that identifies the sending computer as well, what application sent it. There's a destination address and a destination port number, sort of like on an envelope, it's the name and the address together. And then the protocol that's used to transport those packets.

Those five pieces of information will uniquely differentiate one flow of packets on the Internet from

another flow of packets.
Q. And those five pieces of information together can be called a 5-tuple?
A. 5-tuple or "5-tuple."
Q. Another one of those funny names.
Dr. Almeroth, if you would, proceed.
A. Sure. Slide 15 expands out one of these routers or switches, and what it describes is, essentially, the function that one of these routers does. And, at a high level, it's -- the analogy I use with my students is, if you come to an intersection, you have to decide which way to go. If a packet arrives into a router from one of the wires connecting it to a computer or to another router, it will look at the packet payload header, the packet header, and it will determine where that packet should be sent to get it to the destination.
And so, just like in the post office, a letter comes in. You have to decide to put it on a truck to another neighborhood or put it on a plane to go across the country. So based on that address, you figure out where that packet should be sent.
There's a couple of additional terms that come up. Packets come into a router in a place called ingress, and then they leave the router on egress. So you'll hear these terms "ingress" and "egress" being used to describe when

packets come into a router, a decision is made, and then the packets are sent out.

So the animation continues. What I've attempted to do here is kind of drill down into the layers of what happens in the Internet to talk about some of the concepts about moving packets and moving data encryption and what routers and switches do.

The next animation that we get to is kind of just to pop up back to the top level, where you have the businesses, you have the core or backbone of the Internet, and showing that you can have lots of packets being exchanged over this entire network to really drive home the concept of just how much data the world over is being exchanged over the Internet.

Now, in some parts over the first set of my presentation, we've talked a little bit about the evolution of the Internet, and I wanted to focus a little bit on kind of grounding some of what's happening here in the Internet with what's happened over the course of time.

So slide 17 shows a graph, and it shows from the early days of the Internet when, essentially, the web was being developed in about 1992, up until about 2010. And you can imagine, and you've probably witnessed, how the size and speed of the Internet has increased, the complexity of the applications have increased. And, clearly, we're sitting

here now, through the miracle of modern technology, doing Zoom, a trial by Zoom. Things like business transactions, electronic commerce, all of those have, over the last 25 years or so, become very important to our society.

Now, as this graph shows, e-commerce really started to take off in about 1995, and from 1995 until about 2010, there was really a lot of work done to develop new applications and then to also protect the Internet in terms of security.

And I think this case will be about -- and so I don't really want to get into it in the tutorial, but there will be a lot of discussion about exactly what the state-of-the-art was and how much had been accomplished before the patents in this case were filed.

But the point I want to make here on this slide is certainly the evolution of the Internet, which started in 1995, had evolved significantly over the 15 years or so after 1995.

And, with that, slide 18 is the end of the first module, and it really, just in a couple of concise statements, attempts to summarize really the key points I was trying to get across. I'm not going to read them. They're kind of there for your review. If there's any of these statements or anything that I've covered so far that you have more questions about, I'll pause.

THE COURT: No, I think that -- we're up to the point at the end there where it says, "Faster, larger, more complex." That's when we get into the security angle, I guess, at that point.

THE WITNESS: That's true. I think we've -- well, we've been concerned about security for a long time. I think that's something that will come out over the course of the trial.

MR. GAUDET: And, Your Honor, that's exactly the next module we're going to turn to. In fact, the next two relate to security.

So the network security overview, in terms of the types of security approaches that -- and have been taken over time, and then we'll get into sort of a deeper dive into security in the third module, and then the last thing we'll do is talk about the accused products.

So now we're at the network security overview.

BY MR. GAUDET:

Q. Dr. Almeroth, if you would, proceed.

A. Yes. And this is fairly short, and the reason why it's fairly short is because, based on the questions you've asked me and also the questions you asked of Dr. Medvidovic, I think you have a good sense of some of the general aspects of security.

So my first slide on this, slide 20, it's a highly

complex problem. The Internet is very large and complex. There are lots of vulnerabilities that can exist when new software gets developed and deployed. It has bugs that can turn around and be exploited. There's ways of writing software, malware or worms or viruses, all sorts of different software that could go into affecting your computer.

And the point of slide 20 is really just to represent that there's the good guys and the bad guys, and the bad guys are constantly trying to attack networks, to gain information that's supposed to be secure and private, to exploit that information, and there are people who are trying to secure networks, to sell products and services that will protect people from the kinds of attacks that the hackers are attempting to perpetrate.

The concept that I mentioned earlier -- and it also came up in the other tutorial -- is this idea of defense-in-depth. We can use a couple of analogies here, like the courthouse. There's security to gain access to the courthouse. There are court security officers who wander around the courthouse. There are locks on doors so that once you get into the courthouse that doesn't mean that you can just wander anywhere.

The same thing happens throughout our society. At airports, at public buildings, at businesses, you have different levels of security. It's not an expectation that

there will only be one type of security and that it will work perfectly and it will protect everything.

And the same applies for computer security. You can have passwords; you can have software on your computer that will search for viruses. And then the thing that will really be of emphasis here in this trial will be on network security, and the different things that can be done in the network to try and protect users both from giving away their personal information but also to protect private information that's being stored on computers and networks.

Slide 22 shows this same figure, and really the point here is that network security can be implemented in lots of different places in this kind of network. We talked a little bit about the gateway and the routers that exists at the gateway from Dr. Medvidovic's tutorial. You can also use a firewall that gets applied at that point. There's functionality that can be added to routers and switches, and there's software that can be installed on users' computers.

So the point, again, really, is that there is a lot of different places and types of software and types of operations that can be used to try and protect the network.

I bring this point around on slide 23 and introduce kind of two additional points, the first of which is part of implementing security. And some of these challenges have been represented in your questions: How do you do it? What

exactly do you do? When do you implement security? Where do you implement it? And when you combine this with kind of a strategy of defense-in-depth, there's a lot of different options for what you can do in network security.

THE COURT: Well, let's say I'm concerned about the security of my financial information. Sometimes judges have had problems with that, actually, people trying to get their financial information, even though we have to file it, but don't have the details on our bank numbers and so forth.

But if I use my credit card to pay a bill over the Internet, how does the person, the payee, secure it? In other words, if I subscribe to any of these things like Disney or Netflix and I do it over the Internet, unless the person that I'm paying has some sort of security, then it's open to the world, right, my credit card information?

THE WITNESS: That's correct. And they attempt to secure that information, and they do a couple of different things, the first of which is they limit access to the servers that store that information.

They also store that information already encrypted. So if somebody does get access to the computer, they should only get access to the encrypted information. And then what happens is somebody does it badly, and the next thing you know, there is some sort of massive access to information and it shows up in the news. 100,000, 20 million records of

people's credit card information stolen from Equifax, or even a corporation like Sony can be hacked by another country and information from that country stolen, and they can be blackmailed with that, you know, the release of that information. So that's really kind of this give and take of how do we secure this network.

In some cases, hackers gain access to this information because somebody uses their password word "password" and so hackers can just guess what the password is and gain access to their account. And so that's kind of the strategy of why you need defense-in-depth. And from the perspective of this case, you're focused on network security and the things that companies like Cisco and Centripetal can do inside of the network.

THE COURT: To prevent my credit card number or my bank checking account number from being hijacked?

THE WITNESS: That's correct.

THE COURT: And, of course, that depends on the security of the person receiving that information --

THE WITNESS: It does.

THE COURT: -- how secure they are. Because once I send it, I put it out there, so there's no security that I can provide once I send it.

THE WITNESS: That's correct.

THE COURT: I can buy insurance that will reimburse

me if somebody hijacks it, you know.

THE WITNESS: Or your credit card, unrelated to the network, will have fraud protection, and it will monitor the kind of transactions that are happening, and if there's something unusual about the transaction, then it can raise an alert with you.

The transaction was allowed to go through or, in some cases, can be held up, but the credit card companies will mine or analyze large volumes of data to determine whether or not they think that there's some sort of suspicious activity happening. So that would be a different kind of defense-in-depth layer that would be different than, say, protecting packets as they go across the network.

THE COURT: Well, and if an admiral tells the captain of a ship to deploy it to the Mediterranean electronically, then that or whatever that electronic means is has to be secure on both the sender and the receiver's end.

THE WITNESS: That's right.

THE COURT: I mean, that kind of information. All right.

THE WITNESS: One last point to make:

I will add a line on slide 23, and I will change some of the tenses of the verbs, right? The Internet has grown in size and complexity, and on this timeline, up until

2010, there has been significant activity in how to protect networks, lots of products from lots of companies who have tried to develop solutions that will contribute to the different layers of defense. And I think that one of the things that will come out in this case is what some of those network security products are that predated the patents.

With that, that's -- as I said, I promised a short module, and these are the quick summary points before we get into the deep dive.

THE COURT: All right.

MR. GAUDET: Your Honor, the third of the four modules is now a little bit -- as Dr. Almeroth said, a little bit of a deeper dive into the different sorts of ways that you can protect a network, and I think that the credit card example of that is probably a pretty good analogy for a lot of this.

BY MR. GAUDET:

Q. Dr. Almeroth, if you would, proceed with the deeper dive into the network security area.

A. Yes. All right. On slide 27 I'm going to present, basically, two approaches to network security.

Now, these aren't the only approaches that exist. I will come back and describe how these approaches can kind of be mixed together. It's also the case that since you have defense-in-depth, that you can have multiple layers of

security, in fact, some of these approaches working at the same time. But, really, the two approaches are what are described on the screen as packet-based blocking, using inline analysis, and then flow-based allow-and-detect security using out-of-band analysis. Now, the whole point of the next 20 minutes or so will be to give some meaning to those terms.

We've talked about packets, you've heard something about blocking, and you've also seen examples in Dr. Medvidovic's tutorial of inline analysis. So I'll go through that in a fairly straightforward way for the first approach, and then I'll contrast it with the second approach.

Like I try and do, I'll start off with an analogy. So instead of an enterprise network, it's a neighborhood, and the neighborhood wants to implement some form of protection, and they're lucky enough to have a guardhouse. And so cars will approach the guardhouse, just like packets would come into a network, and they will be inspected by the guardhouse. They'll have to pause, answer questions, be checked against a list, but eventually a determination will be made whether or not a car is allowed into the neighborhood or not.

So this is an example of, on a car-by-car basis, a guardhouse is looking at the cars as they pass on the road.

The second car comes up to the gate. It's challenged. It passes the test. It is allowed into the

network.

The third car is not authorized to enter the network. It's not authorized to enter the neighborhood, and so it's prohibited from entering the neighborhood. It's blocked and is not allowed to enter the neighborhood. So that gives you a sense of kind of the basic concept. I want to do that same kind of concept in a computer network and go through those terms of a packet-based blocking system using inline analysis and describe how those terms relate specifically to this computer network.

So now I still have the guardhouse. It might be something like a firewall. It's shown separate from the gateway, so it's functionality that could be implemented into the gateway, but the key here is that the first thing that happens is a series of packets will be sent from some sender in the Internet and be destined for some user in that network.

Now, in each of these packets, I have given it some letters just to differentiate the information that's in the packet. And what the firewall or guardhouse will do is it will use a set of rules where it knows about some packets as being malicious, and if a packet is received and inspected and it doesn't meet one of the rules identifying it as malicious, then it's allowed to proceed into the network, and then it will be routed by the routers and switches, and then

it will reach the destination.

I have another example. Same thing happens. A packet comes in. It's not on the list of rules that would identify it as malicious, and so it's allowed to proceed into the network.

Now, this third packet is on the list of rules and is identified as malicious, and so at that point it's blocked from entering the network. And so using an inline analysis of packets that are coming through the network, they're inspected as they come into the network, and based on whether or not that packet matches a rule, it is either blocked or allowed to proceed into the network.

THE COURT: What happens to the packets that are blocked? Where do they end up?

THE WITNESS: A couple of different things can happen. They can be thrown away virtually, meaning nothing happens to them. They can be rerouted somewhere for some additional inspection.

THE COURT: Well, what do you mean by "nothing happens to them"? They're erased?

THE WITNESS: They're deleted, just like if you delete a file off of your computer. So instead of being allowed to --

THE COURT: But a lot of times you can retrieve what's been deleted, right?

THE WITNESS: Yes. And when you're operating at millions of times a second, there isn't ever really an interest in trying to retrieve these packets that have been blocked or deleted from being forwarded through to the destination.

THE COURT: Well, I don't mean that. I just mean that -- let's say the issue is privacy. You say they're deleted. Does that mean that at some later point they can't be retrieved?

THE WITNESS: That's correct.

THE COURT: That's the theory.

THE WITNESS: That's the theory.

THE COURT: But haven't we had situations where they were found?

THE WITNESS: Usually, if they're found, it's because instead of deleting them, they're redirected for further inspection. They might go to what is called a proxy server, and there they can be stored.

In some cases, you can identify -- you could say, look, this is a bad packet. I want to send it to a proxy server so that it can be inspected.

THE COURT: Well, if somebody were able to get into the guardhouse and look at the guardhouse records, they could find out whatever the guardhouse learned about that packet.

THE WITNESS: That's correct. Who watches the

watcher?

And so somebody else could get into the guardhouse and put in bad rules, and say, you know, "Allow this hacker in." And so part of the layers of defense is to make sure no one gets into the guardhouse who isn't allowed.

BY MR. GAUDET:

Q. So while I fear maybe raising the scary level for the whole notion of a guardhouse, they're rules themselves that reflect known viruses or known malware out on the Internet. Is that generally fair?

A. Yes. That's correct.

Q. And so these things come down and get turned into rules. What happens if one of these companies that supplies that information supplies bad information or bad rules?

A. Two things: You can get what are called false positives, where you think something is bad, but it's not, and so the traffic is actually blocked from the network. That usually results in a user saying, "I was able to get to my e-mail yesterday, but I can't today. What happened?" And so the guardhouse believed something was malicious based on a rule it was given and so blocked that traffic, but it wasn't. So it's called a false positive.

You can also have instances where the rules aren't effective or a piece of malware was just introduced, and so the guardhouse doesn't have the latest set of rules, and so

even if you're using blocking, sometimes malicious packets can get through into the network.

Q. If you would, proceed.

A. Yes. So this kind of packet-based blocking with inline analysis, on slide 30 I prepared a spectrum where you can do simple checks on the red end, the left side, or you can do more detailed inspection on the right side. And this goes to kind of how much inspection that you can do through packet-based blocking using inline analysis.

And I've got a representation. You know, at first you have a very simple guardhouse. As you do more complex processing, where you're looking at more features of a packet, including even looking into the payload to see what data is in the payload, then your guardhouse gets more sophisticated, your device in the network becomes more sophisticated, and then even to the point there's a term called intrusion prevention system. So now it's doing very complex processing of packets to try and understand if these hundred packets all have parts of a malware program and, if they do, being able to block all of those packets.

Now, this gets into kind of a discussion of the pros and cons. It seems like everybody would like guardhouse 3, because you get more protection from an intrusion prevention system than a quick check of a packet header, but the reality is that those kinds of considerations to what happens in the

Internet -- for example, if suddenly the courthouse gets a huge increase in bandwidth, then their guardhouse number 3 may not be able to keep up with the volume of traffic that's coming into the courthouse and to be able to do the complex processing associated with an intrusion prevention system.

And so the who, what, and how, and where of how much processing you can do at the entry point into a network with a device like a firewall will depend on a whole series of characteristics; how much traffic, how much detailed processing of those packets and headers do you want to do, how many rules do you have? The more rules that you have to apply to incoming packets, the more processing speed that you need. If you wanted to process 5 million rules, that would require a lot of capability within that particular device, and that would be a different style of analysis than, say, a firewall with 10,000 rules.

THE COURT: It would need more hardware? Are you saying it would require more hardware or more sophisticated hardware if the software expanded the number of rules?

THE WITNESS: That's exactly correct.

THE COURT: So that's why you try, when you're putting in a new rule, to see if you can erase an old one.

THE WITNESS: That's correct.

THE COURT: In other words, you can't just keep adding, you've got to subtract.

THE WITNESS: And, unfortunately, with more and more applications, you need more and more rules. And so this kind of system is useful in some circumstances, but there's other ways in which security can be implemented.

BY MR. GAUDET:

Q. Dr. Almeroth, you referred to this as an inline analysis, and what does that word "inline" mean?

A. Inline means you're stopping the packets and you're doing the analysis as the packets are coming into the network. So you stop them. You pause them until you can go through all of the rules in the analysis to determine whether or not that packet should be allowed or not.

Q. And Judge Morgan asked a great question in Dr. Medvidovic's -- well, many great questions, but one of them was, are we talking about every packet?

A. Yes, every packet. You can begin to intuit just how much hardware and software you would need to use to get a system to act quickly on all of the packets coming through on a link that has high capacity. Sometimes we call that wire speed. Can the guardhouse operate at wire speed to make sure that packets aren't significantly delayed?

Almost regardless of how much processing you do, you will introduce some amount of delay. In fact, I'm kind of previewing what's on slide 31, which is kind of the pros and cons of packet-based blocking using inline analysis. The

most significant pro here is that you can block and prevent attacks. You can stop packets, and you can delete them, you can send them somewhere else, and you can keep them from going into the network.

The other thing that you can do with a packet-based blocking system is you can develop rules in an automated fashion. So if you get some sort of -- I think the term that was used, and you asked about it, "threat intelligence." And that threat intelligence results in rules being created, and they can be put into the list of rules that are considered when packets come through across the line.

Q. And that threat intelligence, that's the information that's telling us about known viruses, known malwares, that have already hit or been discovered on the Internet.

A. That's correct.

Now, there are some cons, some of which I think I've alluded to, this idea of false positives; that if the rules aren't dead-on perfect, then sometimes you're blocking packets that should be allowed through.

Regardless of how good your hardware and software is, it will add delay, sometimes called latency, and that extra delay and that extra latency can affect user performance. It can take longer to load your web pages if that firewall is trying to do very complex analysis.

It can be expensive. If you are operating a network

that runs at high speeds, then it will take a very sophisticated piece of equipment, hardware and software, to keep up with that rate of packets, to keep up with the wire speed.

The other thing is a network might have multiple entry points, and so you would need one of these devices at every single entry point to analyze all of the packets coming into that network, and so that can be expensive.

The last point here, as you'll see at the bottom of the slide, automated. Automated is both a pro and a con. To quote a favorite movie, "With great capability comes great responsibility." And so if you're not careful, rules that can generate false positives or add delay can be installed into the list of rules and can actually be a detriment to the network trying to get data through.

All right. Questions?

THE COURT: No. I think it's well explained.

THE WITNESS: Thank you, sir.

One final point: I'm showing this battle continued to evolve and changed the verb tenses again. The Internet continued to grow in size and complexity. The Internet has kept evolving. And so the point of this slide is people who have been trying to attack the Internet have been trying to attack it for 25 years. And people who have been trying to protect it have been trying to protect it for 25 years. This

is not something that's happened in the last ten years. And, again, I think over the course of the trial, both sides will be addressing the question of what exactly existed in the prior art?

So I don't want to turn this tutorial into anything but a tutorial except to recognize that there was significant work in security, and part of that security work was because the Internet was continuing to evolve.

BY MR. GAUDET:

Q. My question was going to be is there another way, big picture, to secure a network besides this sort of guardhouse inline model?

A. Yes. So that was the second one on the list. I'll go back to the neighborhood analogy.

Now we're going to use a technique called flow-based allow-and-detect using out-of-band analysis, and I'll contrast that with what I just described.

So in this example, in the neighborhood, there's no guardhouses, but instead what happens is the houses or sensors are able to monitor things about what's happening in that network.

Now, this kind of monitoring doesn't happen on a per-packet basis. It happens on a flow basis, which is one of the reasons why I wanted to introduce the concept of a flow and that a collection of packets together could be

considered a flow.

What's used to determine whether or not things are happening in this neighborhood that shouldn't happen is what I'll call summary statistics. Those summary statistics would go to someplace like a command center or a monitoring site, and they would look at those statistics and try and make a decision as to what's happening.

The analogy here would be, let's say in the neighborhood ten cars come to my house. Well, that may not be a bad thing, but if it turns out that you also learn that I'm on vacation and there's nobody at the house --

THE COURT: Or you're selling drugs.

MR. GAUDET: Your Honor, after some of his answers to me, I had that same question.

THE WITNESS: I will assume that that was a lower case "you," or it's my brother.

So that would require some additional analysis. It would require potentially gathering additional information, you know, maybe calling me and saying, "Hey, is this legitimate?" Or if it turns out that I'm actually there and I'm having a dinner party, then the answer is, "Yes, it actually is okay."

The real distinction here is you're not looking at packets on an individual basis, you're looking at them as sort of a flow summary level. Kind of the analogy that I

would draw there is the difference between, say, getting a voice recording of a call where you hear what was said back and forth. That would tell you a lot about what was happening if you were able to inspect or listen to the words of the call. That doesn't mean that if you got a phone record when the call was placed -- who called, who received the call, how long the call lasted, how many calls, what time of day the calls were placed -- that that kind of flow-level information wouldn't also be useful for performing some analysis.

THE COURT: So what you're talking about is combining a program that will test phone calls with one that matches the traffic at the guardhouse.

THE WITNESS: You could. You could come up with a defense-in-depth strategy, where you had a firewall and it was inspecting packets inline according to a set of rules and blocking some, but to the extent that that firewall wasn't effective, you could use this other approach, in addition. You could collect summary statistics about what was happening in the network.

THE COURT: Well, what would the number of phone calls have to do with -- I mean, that would somehow have to relate to the traffic that was coming into the same home.

THE WITNESS: Even ignoring a traffic-level analysis, if, for example, it turned out that I was placing a

number of calls to a foreign country, that might be suspicious behavior. It might also not be suspicious behavior; I happen to have business with a company in that particular place.

So kind of the call analogy -- and I think, for example, you can do detective work based on call logs and only call logs, and that might give you a suspicion as to some behavior that would require further investigation. You're not in a situation where you would have the call and the words on the call itself. You're not to that point in the investigation, but you would have some summary statistics that might give you a basis on where to look to determine if something was happening.

BY MR. GAUDET:

Q. Dr. Almeroth, we may have mixed the metaphors along the way, and that may have generated just a little bit of confusion. At least I think I may have lost the stream at some point.

Sticking just with the neighborhood and not thinking about telephone calls, in this analogy of a neighborhood, is there any guardhouse or guardhouse equivalent at all?

A. No, not for just this approach.

Q. Everything comes in, right?

A. Everything comes in; that's correct.

Q. So we haven't prevented anything. After it's come in,

are we now sort of looking in a summary fashion to see what kinds of things are going on to figure out if maybe there's a problem, after it's already come in?

A. Right. So you might -- right. That was the example of how many cars to my house, you know, if you had information about where the cars were coming from, or the time of day. If suddenly cars start arriving at my house from midnight 6:00 a.m., that would be the kind of behavior, kind of the flow-level behavior, that might merit some additional investigation to determine --

THE COURT: Well, how do you measure that without a guardhouse?

THE WITNESS: Well, you can measure that by, for example, having sensors in the network, by having -- say at a stop sign, knowing how many cars had gone by. You know, you don't have the level of inspection that you can do on a packet-by-packet basis and see what's in the car or what's in the trunk, you really just get a set of summary statistics that are collected.

THE COURT: Well, it seems like this would be sort of an after-the-fact investigation.

THE WITNESS: Yes, absolutely.

THE COURT: I mean, if everything just came in, you may base the rule on the fact that there's been a lot of malware coming in, and so you look at where it came in from

and sort of go in reverse and put in the rules --

THE WITNESS: That's right.

THE COURT: -- based on history. It's based on history of the club.

MR. GAUDET: Your Honor, the analogy I was going to draw and I referenced was -- we were talking about the credit card. This is rather than preventing the credit card from being breached in the first place, it's looking at your bill, realizing something bad happened, and then calling your credit card company and invoking your insurance to do something about it; history versus stopping it on the way in.

BY MR. GAUDET:

Q. Dr. Almeroth, is that a fair way of putting it?

A. Yes. It is absolutely after the fact. I think that's an important point to keep in mind.

Q. And, in fact, by the time -- and we'll go into the specific -- we'll get rid of the analogy and go into the specific technology, but I think this is an important point to raise here:

By the time that summary information is even sent to anybody who can do something with it, what's happened to the packet that may have -- or the packets that have generated that summary information?

A. They're already at the destination. You have allowed the packets to go through. That's the second part of it. You've

allowed them to go through, and you want to do the post facto analysis to determine if you can detect something.

Q. Let's proceed and actually move away from the analogy and into the specific technology.

A. All right. So now we have this computer figure again. I've introduced, on the right side, this flow collection and analysis device with the person sitting there. The first step that will happen is that information from all of the routers and switches, kind of this summary statistics using a technique called NetFlow, which is flow summary information which is collected at the routers and switches, that summary information would be sent to that flow collection and analysis device.

To show that in a little bit more detail, I have an animation, and the animation will show a sender, located on the other side of the Internet, that goes through one router or switch that we can collect data from and then on to the receiver. And so these packets come through the network.

Now, understanding again one of the last things that we talked about, there can be millions of packets, and operating at line speed or wire speed, it can be millions of packets in every second. And the point that the router can do is it can collect a flow summary for the different flows that go through that router, and it can send just that summary to the flow collection and analysis device.

And that flow summary might include things --
Q. Doctor, I want to stop you there just to be sure we're clear about the graphic.
The words "600 packets" was on that thing that kind of went up there. Are the packets themselves ever going up to the flow collection analysis?
A. No, just the summary. I mean, you can imagine if you made copies of all of the packets and then sent copies of all of the packets through the network and then you had to monitor the copies of all of the packets and then copy all of the packets that were copies, you can really only do the summary.
Q. Okay.
A. So that summary goes up to the flow collection analysis.
THE COURT: I want the attorneys to get that point.
MR. GAUDET: Your Honor, I told Mr. Jameson he shouldn't have done that.
THE COURT: I want to control the flow collection.
MR. GAUDET: We got it loud and clear.
THE WITNESS: Probably what Your Honor would not like to see is that there then is another flow summary that comes in that adds additional information on the original flow summary. And so, at least in the network context, these flow summaries can come in periodically. They're not the packets. So it just summarizes the flow.

I mentioned in that original figure that in the Internet, networking and monitoring, that the way that you summarize these flows and the types of information is according to something called NetFlow.

NetFlow is an Internet Engineering Task Force standard. It was published in October 2004. It actually originated with Cisco, I think, in the late '90s, but it became an Internet standard that everyone could use to describe kind of the way that you could put statistics into a flow summary.

Because the point is you want these flow summaries to be accessible by any kind of flow collection and analysis system, and because it doesn't have to be in the network, it's important to have a standard to represent kind of who's communicating, when, and what, and how much, and for how long, so that any kind of flow collection and analysis system can use those flow summaries to do some after-the-fact analysis.

BY MR. GAUDET:

Q. In terms of the after-the-fact analysis, you know, we've used analogies so far like cars coming to your house, that sort of thing, but in the real world, would this be -- for example, we see that an extraordinarily large number of packets is going to or coming out of some particular device, that that almost never happens, and that must be trouble. Is

it something like that?
A. That's correct. So, Mr. Gaudet, you're getting into the phase of what do you do with those flow summaries, so really the next step, sort of back to this representation of the real network, is that there's an inspection that takes place to try and mine all of that summary data to see if there's anything worth understanding out of that data.

And so there's this offline phase where you're looking at all of these statistics that can be collected from the network. In fact, sometimes the word -- I saw it in one of the documents that Dr. Medvidovic presented -- is called telemetry. So you have telemetry information and summary statistics that could be mined and analyzed, and ultimately some of that data could potentially indicate that there's something that merits further investigation.

So an e-mail comes through, and it's allowed into the system, and the e-mail says: Hey, this is your credit card company. Something bad has happened. Click on this link and enter all of your private information.

Well, that e-mail didn't come from the credit card company, but, as a result, somebody looked at that e-mail, clicked on the link, and now they've started communicating over time with some other company in a different part of the world.

And somebody would look at that and say, wait a

second. This person doesn't normally communicate with this other country, they communicate with their own bank. I should look and see what kinds of flow statistics there are to see whether or not that person hasn't actually been tricked into entering their information, their private information, and giving it away to somebody else. But it happens after the fact, based on the summary statistics.

Q. And one other just clarifying point:

I think you used the word -- or over the course of the proceedings today, we've heard the words telemetry, flow data, and NetFlow, and are those all talking about the same thing, just summary information?

A. That's correct.

Q. Okay. Summary information, but that's not the packets themselves?

A. That is not the packets themselves.

And, again, that makes sense. You see in slide 37 that you're getting lots of telemetry or NetFlow data from the different routers and switches. You can't create copies of all of those packets that the routers and switches are doing. It would just place too much of a burden on the network to try and deliver copies of packets at every router and switch seat, so you have to kind of bump up the level of abstraction so that you're getting not the details of the packets but the summaries of the flows.

Pros and cons here. There's a number of pros. It's not a bottleneck. You can do lots of analysis. That magnifying glass was rotating around constantly. You can take as long as you want to do the analysis. You have more time. You're not slowing packets down. You're not introducing delays in latency. Because you're not blocking packets, you don't delete packets or remove them because of false positives. You allow the packets through and then do some detection, and so it doesn't introduce delays and latency.

Now, there's a big con here, which is you can't block or filter packets. You have to respond to the threats after those packets have been received and after whatever was going to happen with those packets has been done. So that's why it's an allow-and-detect strategy as opposed to a blocking strategy. And it's done out-of-band, so it doesn't introduce the delays and the bottlenecks that inline analysis does.

Q. And two questions:

The phrase "out-of-band," is that simply to contrast with "inline," where inline means you're in the line of the network traffic, and out-of-band means you're sort of outside, looking in?

A. That's correct.

Q. And then last question:

For a defense-in-depth strategy, could you do some combination of these different things?

A. Absolutely. And that points to kind of the give-and-take between the attackers and those who secure the network and the who, what, when, where, and how; that you can protect a network through multiple layers, and each of those layers is designed to do different things, has different pros and cons, provides different levels of protection, cost different amounts of money. So depending on how much money you want to dedicate to protecting your network and how important that data is, then you can allocate more budget to securing your network.

Q. Why don't we just briefly talk about one other possibility here.

MR. GAUDET: Then, Your Honor, we will turn to the accused products and, with that, finally, land this plane, so to speak.

THE WITNESS: So there's a third approach to consider, just to kind of round out how this works. And I'll do this very quickly.

I've created slide 40, which shows you what it looks like. Many of the same words are there, but it's a packet-based, allow-and-detect doing out-of-band analysis, so it has similarities and flavors to each of these.

Packet-based is allow-and-detect, and it's

out-of-band. So slide 41 gives you an example of what it looks like, and the key piece here is the use of a new piece of equipment called a tap. And I have an animation that will walk through this to kind of describe how this works.

And I'll do the first click, because what it shows is a packet coming into the network, and what that tap does is it creates a duplicate of that packet. It allows the packet to continue through but at the same time makes a copy that it passes up to what's called an intrusion detection system.

It's different than an intrusion prevention system, because even if that packet is determined to be malicious, it's already allowed the original version of that packet through into the network.

THE COURT: Well, how would you do that, if it was encrypted?

THE WITNESS: So if it was encrypted, then you would have to apply different kinds of rules. And I think you questioned Dr. Medvidovic about this, in terms of, you know, maybe you could look at the size of the packet. Well, then the attacker says, "I'll just obscure how big the packet is by adding some extra steps." And then you say, "Well, I'll figure out where it's coming from." And the attacker says, "Well, I can fake where it's coming from."

So it's this back-and-forth about what kind of

information that you can use to really determine what's happening.

And as soon as you have rules for this kind of thing, then sometimes the hackers can find ways of getting packets through that are malicious but haven't been detected or can't be detected by...

THE COURT: You'd have to get a search warrant for the receiver.

THE WITNESS: Eventually, you might have to. If you do the offline analysis and it's effective and thorough, it might point to a real problem that you have to then...

THE COURT: They say that your testimony is trailing off. She can't hear the ending.

THE WITNESS: Yes, sir. I will not trail off.

BY MR. GAUDET:

Q. I think it's started about the time that Judge Morgan revealed you as a drug dealer.

A. So to review the technology here, the tap makes a copy of packets, and then the packet, the original packet, is allowed to the destination. The duplicated packet goes up to the guardhouse for inspection. So I paused it there, and now I'll show that the original packet goes through, and the duplicated packet goes up for inspection.

I'll show a second packet without a slip to just show that it's duplicated, analyzed, but at the same time

allowed to go through.

I'll show a third packet that's duplicated, allowed to go through, but matches a rule and is determined to be malicious.

So this is a packet-based system. It looks at individual packets. It works by doing allow-and-detect, because it doesn't block packets that it determines to be malicious; it allows them through. And it does out-of-band analysis because the guardhouse is not in-band, inline, doing the inspection.

So it's kind of a third approach that mixes and matches some of these different kinds of techniques, and so there's a different set of pros and cons. It's not a bottleneck. You don't block on false positives. It doesn't introduce the kinds of delays and latencies that inline analysis would do.

The pro here of the tap is that you also get a copy of all of the packets, and so you can do that same kind of packet-by-packet analysis that firewalls could do. But there are cons to that.

Just like the flow-based allow-and-detect, you can't block and filter. You're doing this kind of offline analysis after the fact. And even though you're getting all of the packets, you're getting all of the packets, so you have to do the analysis on all of the packets. And that means that it's

going to be expensive and require a lot of hardware and software, and if you want to do a lot of complex processing, it will be very expensive to do on those copies of the packets.

But, as you alluded to earlier, these different approaches can be combined in different ways to create a defense-in-depth strategy. So depending on products that are available, you can use different techniques in combination. You can use different strength techniques at different places in your network, depending on how you want to be able to detect that.

MR. GAUDET: Your Honor, our fourth and final module is the accused products.

And Dr. Medvidovic -- the same products that he talked about, one of the main takeaways here, Your Honor, is, as Dr. Medvidovic put up the various products, he had the same kind of a line drawn between all of them, almost -- and I don't know that he intended this, but you could be led to believe that the network traffic was actually going between all of these different products.

I think, as we get into this case, it's very important to see where the network traffic packets are and what's actually going between the various products, and so in our images, we try to differentiate that based on the different kinds of lines that we're going to show. I just

say that by way of general background.
BY MR. GAUDET:
Q. And, Dr. Almeroth, if you could, give us a sort of roadmapping of the accused products and how these things will interrelate with each other.
A. Yes. My intention in this overview is really just to say what some of the names are and to identify the acronyms. I think over the course of this trial, it will become clear what those products actually do, and so I want to be very careful to keep this at a tutorial level.
So the first line on slide 44 is to identify the accused firewalls, routers, and switches, and these are the same things that Dr. Medvidovic pointed to; the catalyst switches, the Aggregation Service Routers, the Integrated Service Routers, and then the Adaptive Security Appliance.
THE COURT: The first one, it says catalyst switches. Did you name that?
MR. GAUDET: Your Honor, I think that's actually showing a stack of multiple switches. That's why it's plural there, if that was your question.
THE COURT: My question was are you counting the switches as a firewall?
THE WITNESS: No.
THE COURT: It says, "Accused firewalls, routers, and switches." Okay. So the switches --

MR. GAUDET: We've got it in exactly the opposite order, Your Honor. We apologize for that. It actually goes switches, routers, firewalls.

THE COURT: All right. Just a second.

It's got two kinds of routers, and the fourth, the Adaptive Security Appliance, is a firewall. Is that what you mean?

THE WITNESS: Yes. Yes.

If you don't mind, Your Honor, let me skip ahead two slides. The way that I've organized this description is I've actually put into words kind of a summary of what each of these are so that if you wanted, you could go back and review kind of a quick summary as to what a catalyst switch is versus, say, an Aggregation Services Router.

And so you'll see that, for example, the Adaptive Security Appliance -- that's described there. It provides what's called FirePower service, which is a kind of firewall. And so these words, I think, should help guide you, if you kind of need a glossary later in the trial as to which are the switches and which are the routers and which are the firewalls.

THE COURT: Okay.

THE WITNESS: I'll go back one slide. I've highlighted in orange where these products would exist in kind of this representative network that I've come to a few

times.

So the routers and switches could connect the users to other users or to other routers and switches or servers, and then the firewall could potentially sit at the gateway or beyond the gateway.

Now, the next two slides will talk about some additional management devices. Dr. Medvidovic also described these. All I really want to do in this tutorial is to identify the name and the acronym and, at a very high level, give a very brief description of the kinds of things that it does. Again, I think if I started to describe how these devices would work in detail, it would start to sound like testimony.

So the purpose of this part of the tutorial -- there will be a slide after this one that has lots of words on it, and those words will summarize kind of the basic functionality of each of the devices that will be listed here.

So, at a very high level, the Digital Network Architecture center will be used by somebody, a network administrator, who could configure a router or switch.

BY MR. GAUDET:

Q. Dr. Almeroth, again, this is the IT person, for example, that had us all set up our equipment to make this trial possible, correct?

A. That's correct. That's what, half a dozen, ten or so people that are working very hard to make this trial come off over Zoom?

THE COURT: So the DNA controls the switches, routers, and firewalls, all three?

THE WITNESS: That's correct. So let me jump ahead to slide 48. You'll see that summary there.

It's an IT manager's device for setting up and maintaining the switch and routers of the network.

THE COURT: All right. So "DNA" stands for what?

THE WITNESS: Digital Network Architecture.

MR. GAUDET: And, Your Honor, just one point of clarification:

The line from DNA actually does not go out to the firewall. In other words, there's a different piece of equipment that will control the firewall.

THE COURT: What's the third -- what is the "A" in DNA?

THE WITNESS: Architecture.

THE COURT: Okay.

THE WITNESS: Let me give you a quick example.

A Digital Network Architecture center would be really useful in a network that might have hundreds of switches and routers in it. And so if a new network or a new switch or router were added to that network, say, a 60-story

building with lots of routers and switches, DNA would be useful for configuring that router so that it would operate on that particular network.

So it's, you know, making sure that it has routing information to get to other destinations, setting up passwords, and those kinds of functions.

THE COURT: Well, so there are no firewalls here. The only thing this illustrates is how the DNA controls the switches and routers.

THE WITNESS: It gives them the configuration so they can operate; that's correct.

THE COURT: So that's just sort of an operating system, not a security system, correct?

THE WITNESS: That's correct.

THE COURT: Okay. All right.

THE WITNESS: Now, the second one is called the Identity Services Engine. And, again, I will jump to slide 48 and show you that I've given you some words that you can come back and reference.

It's a management device for tracking identity of users and user computers on a network and for setting the limits of user and user computer access to other devices on the network.

And let me give you a little bit of an analogy to help you understand kind of what an Identity Services Engine

might do.

So, for example, in the courthouse, you have badges for employees and for visitors. We talked about that router and switch for users 1, 2, and 3. The Identity Services Engine would be used to establish a group that would say only employees, only people who are inside of this network, can communicate with users 1, 2, and 3, and visitors could only access servers 1 and 2. And so the router and the switch would be able to use those groups in order to identify packets as being part of that group and, therefore, allowed into the network or not. And so the Identity Services Engine, this management device, is the thing that would allow those groups to be configured in that router and switch.

THE COURT: All right.

THE WITNESS: The reason why you have the separate device like this is so that, say, in the courthouse, if 10 new badges are being used for visitors and so they have numbers that are in the range not currently being allowed into the visitor space, you wouldn't want somebody to have to go around to all of the places where those badges could be used and start changing every single place every badge is used.

Same thing in a network. If an additional router or switch comes online and it needs to be configured, or the number of visitor badges or people who can access certain

portions of the network change, then you can use the Identity Services Engine to change those configurations without having to go to each router or switch individually. That's something that that management device would do for you.

THE COURT: All right.

THE WITNESS: The third piece on this slide 47 is called the FirePower Management Center. And now I've added the Adaptive Security Appliance or the Adaptive Security Appliance with FirePower Services or a FirePower appliance. They can be separate things.

THE COURT: Wait a minute.

THE WITNESS: But what the FirePower Management Center does --

THE COURT: Wait a minute. ASR means --

THE WITNESS: ASA.

THE COURT: ASA?

THE WITNESS: Yes, sir.

THE COURT: All right. "ASA" means what?

THE WITNESS: That is the Adaptive Security Appliance. And I will show you on the next slide. That has the summary.

It's an inline security product with advanced packet-filtering functionality, about that fourth row I'm reading from. And there's a portion of that Adaptive Security Appliance called the FirePower Services. So it's

FirePower Services within the Adaptive Security Appliance, and that portion is managed by what's called the FirePower Management Center.

BY MR. GAUDET:

Q. Dr. Almeroth, just to back up just a little bit, this is the firewall, right?

A. Yes, this is the firewall.

Q. The Adaptive Security Appliance, the FirePower Services, or the FirePower appliance, whatever, that is the inline firewall?

A. Yes, sir.

THE COURT: All right. It's not a firewall until you add the Adaptive Security Appliance to the router.

THE WITNESS: Well, the Adaptive Security appliance is the firewall. I think that the reason why there's a couple of different components is because this has been a product that Cisco has offered for a very long time, and so it has to be described this way, as different.

MR. GAUDET: And let me just maybe put it this way:

On this image, Your Honor, the only place that there's a firewall is that far left. Right after the Internet, it's got the wall and the little fire, and that list of names are the different sort of kinds of appliances that are the firewalls.

And then the thing on the right side, the FirePower

Management Center, that's the thing that the court staff, the network manager, the IT staff, uses to control the firewall over on the left side of the screen.

BY MR. GAUDET:

Q. Dr. Almeroth, is that a fair description?

A. That's correct. The management center is like the other management devices. It can be located remotely and then be used to configure or manage that firewall.

Q. And let me ask a couple more general questions.

Everything on the right that says "management devices," are any of those things inline, meaning that they're actually getting the network traffic or seeing the packets that are coming into the network?

A. No. They're management devices. They sit out of band. And, also, in these particular cases, these types of devices are mostly used for management. So they're used for configuring the routers or switches, in the first two instances, or the firewall in the third instance.

THE COURT: Okay.

THE WITNESS: All right. Again, this slide 48 summarizes kind of these words. So as you come to understand what these products do or need a refresher, then that's where they will exist.

So the next is to talk about the additional set of management devices that are also accused. So the first is

what's called Stealthwatch. One of the other terms that you will hear in the context of infringement allegations is the idea of NetFlow. And NetFlow is what I described earlier. It's that standard from the IETF. That's what creates the flow summaries that are used by the accused Stealthwatch product.

Stealthwatch is what receives those summaries and is able to do analysis of those summaries to create alerts that something strange is happening, based on all of the network statistics that it is able to gather. And I've used statistics, NetFlow summaries, and telemetry.

But the next step of this animation shows that --

BY MR. GAUDET:

Q. Dr. Almeroth, before we go there, is this -- and we talked about the two different types of network approaches. There was the guardhouse, and then there was the allow-and-detect, after-the-fact look at summaries and see if something bad happened. Which one is this?

THE COURT: After the fact.

THE WITNESS: This is just what the title says; it's flow-based, it's allow-and-detect, and it's out-of-band analysis. So it doesn't look at packets, it doesn't do blocking, and it doesn't operate inline.

The next part of this animation, to show how it works with other products, is you do an analysis of that

data, and if something suspicious happens, then an alert can be presented on a screen to a user.

Now, I'll pause for a second.

What also happens is that the Stealthwatch information can be passed to what's called Cognitive Threat Analytics, or CTA. This is shown as being remote even from Stealthwatch and from the network. This is also out-of-band, and I believe you'll hear testimony that CTA is performed, actually, overseas.

Now, CTA can use the information that it's given, the NetFlow records, to do its own analysis. And it, too, in addition to alerts that can be generated by Stealthwatch, might also generate an alert, and that can be displayed on a dashboard to a user.

So, for example, let's say you have the IT staff in the courthouse. They can be in their office. They can have on their screen that you would get certain kinds of alerts. Those alerts might come from a Stealthwatch device, or they might come from Cognitive Threat Analytics that happen not even in the courthouse. So information can be passed and then additional analysis can be done.

BY MR. GAUDET:

Q. Dr. Almeroth, just to maybe step through that, because I know this is a point that sometimes in the details can get a little thick, so to speak.

Cognitive Threat Analytics, if it looks at this same NetFlow information, this is, what, another tool to analyze NetFlow information that can also send an alert up to Stealthwatch? Is that a fair way of saying that?

A. That's correct.

Q. And then once you get these alerts at Stealthwatch, it is literally a human -- not this human, because I wouldn't know what to do with them -- but an IT staff member, a manager, who would look at them, at those alerts, and decide either it's no big deal or maybe I want to do something about it.

A. That's correct. And, using the credit card analogy, you would get all of this information, and somebody might look at that information and decide that it was worth putting a block on your credit card, or that something suspicious had happened, and they might call you up and say, were you really in Washington, D.C. on these dates?

And so there's CTA, as you described it, and then there's also the Encrypted Traffic Analytics. So there's portions of the encrypted traffic that can be provided as part of NetFlow. And when I -- portions related to the summary of the encrypted packet flow, not anything about the packets themselves or, as we've discussed, the data encrypted that's not useful to analyze.

THE COURT: This is after the fact.

THE WITNESS: All of this is after the fact, Your

Honor, absolutely.

THE COURT: Everything in Stealthwatch is?

THE WITNESS: Yes, sir.

BY MR. GAUDET:

Q. And so is it fair to think of Cognitive Threat Analytics and Encrypted Traffic Analytics as a couple of tools that you can use after the fact, with Stealthwatch, in order to analyze these NetFlow summaries of what's already happened?

A. Yes. It's different animals of the same type, right? Stealthwatch can do its own analysis. That was the revolving magnifying glass. CTA can do its own analysis. That was part of that revolving magnifying glass. ETA can do its own analysis.

It's almost like the more people, the more techniques, that can be applied to this data, the more potential alerts and the more detailed information that can be determined.

This is offline. So you have ample opportunity to sift through all of those summary statistics to try and just tease out that there's something suspicious happening. And the result of these Cisco products -- Stealthwatch, CTA, and ETA -- is to put alerts onto a dashboard, onto a screen, that would say to somebody, you know, there's something that's atypical. This is unusual. The volumes of traffic, where the flows are coming from, the durations of the flows are

just atypical. There's something that's not right here.
Q. Two quick points I want to be clear about. We actually added -- there's the NetFlow blue dot that indicates these summaries that are going from the gateways and routers over to Stealthwatch, and we added with ETA.

Now, is that just indicating we're sending a couple of additional fields of information with the NetFlow summary? Just a little more information?
A. Yes, some additional summary information related to the security pieces.
Q. Now, at a very high level, I think in the prior tutorial, there is a suggestion that --

THE COURT: What is ETA? Encrypted Traffic Analytics?

MR. GAUDET: That's correct, Your Honor. That's entirely on me. I should have spelled that out.

THE COURT: Just a second.

(There was a pause in the proceedings.)

THE COURT: Okay.

BY MR. GAUDET:
Q. In Dr. Medvidovic's tutorial, he showed sort of an ETA icon on, for example, all the routers and switches, and he made a statement. And I think he meant this at a very high level. I don't think he meant to mislead anyone, but he said there's a copy of Encrypted Traffic Analytics, or ETA, at

every router and switch.

Now, there's no copy of this software that the human is interacting with over the rights in the management devices at these routers and switches, is there?

A. No, absolutely not. What those routers and switches can do is generate summary statistics that include fields and information that ETA can use. All of this is out-of-band management devices. These are not things that happen in-band or in-blocking. This is all under the philosophy of doing analysis after the fact.

Q. So by the time that Stealthwatch gets information, what's happened to the packet that is being summarized?

A. It's already arrived at its destination.

Q. Thank you, Doctor. If you would, proceed.

MR. GAUDET: I think we're almost done, Your Honor.

THE COURT: Did the doctor go to the beach this weekend, disobeying what the Governor said out there?

MR. GAUDET: I think it's the lighting. We're planning to recall Dr. Almeroth, and he might just tell us, "No," after this.

THE COURT: Certainly looks like he got a little sun. But, anyway...

THE WITNESS: You know, Your Honor, I will take a picture and e-mail it to you, because I don't know if it's the lighting in this room or exactly what, but I am neither

this red nor this embarrassed.

THE COURT: All right.

THE WITNESS: All right. There's one tiny animation that happens on the right side, and that's where the eureka moment happens, where the network, the IT manager, says, "Oh, my goodness. Somebody sent a virus to Judge Morgan, and now it's on his computer." And it's already on your computer, and so he'd have to run in and try and get it removed. But again, it all happens after the fact.

In some cases, one of the things that that IT manager can do is go back and use the Identity Services Engine in the network to prevent any further infiltration of that particular device. So there's an additional slide that shows one of the things that you can do is, in order to protect the network, you've withdrawn access for user 6. You've removed them from the trusted group, just like ICE can do as part of its identity services and remove people from the group.

It's almost like saying, "Badge No. 10, we're going to take you out of the employee pool and remove you and put you in the guest pool." And so you can control access to the network by reconfiguring the network through the use of Identity Services Engine.

THE COURT: This is adding a rule. Is that what that is, if you do that?

THE WITNESS: The rules or the group already exist. You would be adding a member to that group.

BY MR. GAUDET:

Q. Let me put it this way: Are quarantines all or nothing?

A. No.

Q. In other words, when you quarantine, although the quarantined user can still communicate with the IT staff -- right -- other communications are all shut off at that point?

A. That's correct.

Q. Yeah. So the exception to the "all or nothing" is the staff, but at this point, are you saying, well, they can get packets, certain kinds of packets, but not other packets, we'll look at this rule, but it's not that rule, or is it just you're quarantined?

A. You would be quarantined.

Q. Is it a fair analogy to say, sort of like with the credit card, if you know that only one person has stolen your credit card -- right -- you still have to get rid of the account in total, and nobody can use the credit card anymore, as opposed to figuring out what the charges are for that specific person?

A. That's correct.

Q. Okay.

A. You'd suspend access to the credit card.

THE WITNESS: And again, Your Honor, slide 52 gives

you some words to go along with these particular components. Identity Services Engine, I already described. So this adds the description of Stealthwatch enterprise, the Cognitive Threat Analytics, and then also the Encrypted Traffic Analytics, in case you want to come back and see a brief summary of the products that have been accused.

And with that, the last and most important slide, I'm done.

THE COURT: Well, I'm glad it's the last one, because I'm going to need more hardware to deal with any other information today.

THE WITNESS: The fact that you're still with me, Your Honor, is something I'm surprised by.

THE COURT: All right. Well, that completes your tutorial?

THE WITNESS: Yes, sir.

MR. GAUDET: Your Honor, that's the last thing we have from Cisco on the tutorial. Thank you very much.

THE COURT: All right. Well, I think the tutorials have been very helpful in understanding the basics of what we're talking about, but translating the basics into the words of the claims and how the defending products operate I have a feeling is going to be more complex.

Well, we thought that we might get the opening statements done today, which we obviously are not.

Is there anything else that we need to take up today?

MR. ANDRE: Your Honor, for Centripetal, there's nothing to take up today. I think we can start the opening statements tomorrow morning and then start doing the presentation of evidence with our first witnesses.

THE COURT: All right.

MR. GAUDET: Nothing for Cisco, Your Honor.

THE COURT: All right. Will we have what we discussed about the outline of the factual areas of the witnesses' testimony tomorrow?

MR. ANDRE: Yes, Your Honor. We had already provided the witness binders to the Court for the first two witnesses we thought we might get on today. We will supplement those tomorrow morning with the summary that you asked for.

THE COURT: All right. And the same thing for cross-examination. I don't know whether -- it's not as easy to do it for cross-examination as it is for the proponent witness, but I'm sure that the defense has mapped out areas of cross-examination, so I would like to have those before the cross-examination begins.

MR. GAUDET: It will be our plan to get those to you in the same time frame that Mr. Andre mentioned of supplementing our existing cross-examination binders, and

then we'll just provide that information over to Centripetal right before the cross-examination begins.

THE COURT: Right. If there's nothing further, then we will be adjourned for the day.

MR. ANDRE: Thank you, Your Honor.

MR. GAUDET: Thank you, Your Honor.

(Off the record at 3:59 p.m.)

CERTIFICATION

I certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

_____/s/_____

Carol L. Naughton

May 6, 2020